JEFFREY D. GOOCH (7863)
J. ANGUS EDWARDS (4563)
JONES WALDO HOLBROOK & MCDONOUGH, P.C.
170 South Main Street, Suite 1500
Salt Lake City, Utah 84101
Tel.: (801) 521-3200
jgooch@joneswaldo.com
aedwards@joneswaldo.com

Attorneys for the Seavers

IN THE UNITED STATES DISTRICT COURT

DISTRICT OF UTAH, CENTRAL DIVISION

JAMES SEAVER and DEBORAH SEAVER, as parents and heirs of G.S., deceased, Plaintiffs, v. The ESTATE of ALEXANDRE CAZES, deceased, a citizen of Canada, formerly doing business as ALPHABAY; THE TOR PROJECT, INC. aka THE ONION ROUTER, a Massachusetts non-profit corporation; CHINA POSTAL EXPRESS & LOGISTICS COMPANY aka CHINA POST aka CHINA COURIER SERVICES CORPORATION, a Chinese corporate or governmental entity; and EMS COOPERATIVE dba EXPRESS MAIL SERVICE, a foreign entity, Defendants.	**PLAINTIFFS' OPPOSITION TO TOR'S MOTION TO DISMISS** Case No.: 2:18-cv-00712-DB-DBP Judge Dee Benson Magistrate Judge Dustin B. Pead

In accordance with Rule 7 of the Federal Rules of Civil Procedure and local rule DUCivR 7-1(b), Plaintiffs James and Deborah Seaver ("the Seavers") respectfully submit this opposition to the Motion to Dismiss filed by Defendant The Tor Project, Inc. ("Tor").

Preferred Disposition

The Court should deny Tor's motion. Tor is not a brick-and-mortar store in some other state whose only connection to Utah is a web portal, nor is it some type of online hosting site where "user content" is circulated. Tor is an online anonymity-granting service, that relies both on a program—software that encrypts transmissions and strips identifying information in stages—and on a network—thousands and thousands of users, relays, and bridges, "nodes" connected by "tunnels," through which information passes. Tor's anonymizing features make mapping the exact network impossible in practice, particularly at the outset of a case. But there's little doubt that Tor's network operates through users and relays in Utah—Tor's own website encourages all visitors to download the Tor browser and to set up the relays that make Tor's services powerful.

In its Motion to Dismiss, Tor argues that it's not subject to either general or specific jurisdiction here in Utah, that it's immune from suit under the Communications Decency Act, and that the death of the Seavers' son—from synthetic opioids whose path from a Chinese lab to the hands of Park City middle schoolers was possible only because of Tor's anonymizing services—is not "traceable" to Tor.[1] All three of Tor's arguments fail, for the reasons provided below, and the Court should therefore deny Tor's Motion to Dismiss.

Background Facts

In early 2018, the U.S. Senate's Permanent Subcommittee on Investigations issued a lengthy, heavily sourced report titled, "Combatting the Opioid Crisis: Exploiting Vulnerabilities in

[1] Tor appears to fundamentally misunderstand one important aspect of the Seavers' Complaint. Tor states, on more than one occasion, that it was *the Seavers' son*—G.S.—who used Tor in bringing opioids into the U.S. *See* Tor's Mot. to Dismiss, at 2 [Dkt. 13] ("Plaintiff's Complaint alleges that [the] Seavers' minor son, G.S., used the Tor Browser to access the AlphaBay website to purchase U-47700."); *id.* at 12 ("Plaintiff's allegations relating to Tor are that it acted as a publisher or speaker of the website *that G.S. viewed and interacted with to purchase U-47700*."); *id.* at 13 ("Tor did not create or contribute to the content *that G.S. viewed*.); *id.* at 14 ("Tor was the web-browser that displayed the website from which G.S. allegedly purchased the U-47700."); *see also* Steele Decl. ¶ 5 [Dkt. 13-1) ("The Tor Browser and network . . . can be used for illicit purposes, *such as what G.S. used it for*.).

This is *not* what the Seavers' Complaint alleges. Rather, the Seavers allege that "shortly before [their son's] death, *two of his friends*, minor children C.S. and J.A., purchased U-47700 from China using AlphaBay." *See* Compl. ¶ 17 [Dkt. 2]; *id.* at ¶¶ 33–36 (stating that "the Defendants shipped, marketed, distributed, sold, and/or transported the U-47700 *to C.S. and J.A.*," not to the Seavers' son G.S.).

International Mail."[2] Based on the findings of that report, the path that the potent synthetic opioids that killed the Seavers' son took on their way to the United States was a well-worn one: they were manufactured in a Chinese lab, purchased using cryptocurrency, shipped through Express Mail Service rather than "Express Consignment Operators" (like DHL, FedEx, and UPS), and—most critically for the purposes of this opposition—sold "openly on the internet," using Tor to hide the identities of those in the supply chain. *See* Senate Opioid Report 8–9, 18–19 & nn. 37–38.

Tor insists that it is an "internet company," and presses into service ill-fitting caselaw. A widget-maker doesn't subject itself to worldwide personal jurisdiction just by making a website, Tor reasons, and therefore Tor can't be sued in Utah—even if it played a critical role in G.S.'s death. And an online bulletin board shouldn't be liable for defamatory statements posted by a user, Tor reasons, and therefore Tor shouldn't be liable for its role in G.S.'s death.

But Tor isn't a widget-maker hawking its wares to an internet audience or an online publisher acting as a conduit through which content providers speak. Tor is an "online anonymity-granting system," a foundational building block for the Dark Web. *See* Eric Jardine, Global Comm'n on Internet Governance, *The Dark Web Dilemma: Tor Anonymity and Online Policing* 1 (2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2667711.[3] As one recent study concluded, "The Tor network is a relatively unknown and unexplored region of the dark web allowing users to anonymously communicate and browse content through encrypted means." Bryan Monk et al.,

[2] The report is readily accessible online. *See* U.S. Sen. Comm. on Homeland Sec. & Gov't Affairs, Permanent Subcommittee on Investigations, *Combatting the Opioid Crisis: Exploiting Vulnerabilities in International Mail* (2018) (hereafter, "Senate Opioid Report"), https://www.hsgac.senate.gov/imo/media/doc/Combatting%20the%20Opioid%20Crisis%20-%20Exploiting%20Vulnerabilities%20in%20International%20Mail1.pdf.

[3] An early paper similarly described Tor as "a circuit-based low-latency anonymous communication service," which "works on the real-world Internet, requires no special privileges or kernel modifications, requires little synchronization or coordination between nodes, and provides a reasonable tradeoff between anonymity, usability, and efficiency." Roger Dingledine, et al., *Tor: The Second-Generation Onion Router* (2004), https://www.nrl.navy.mil/itd/chacs/sites/www.nrl.navy.mil.itd.chacs/files/pdfs/Dingledine%20etal2004.pdf.

Uncovering Tor: An Examination of the Network Structure, Security & Commc'n Networks (2018), https://www.hindawi.com/journals/scn/2018/4231326/ref/.

One simple comparison likens Tor to "the children's game of telephone," anonymizing users at either end of a network by passing information though other intermediary users:

> Tor accesses information on the Web in much the same way, but it breaks up the direct connection. After a fashion, the Tor browser is a bit like an anonymous version of the children's game of telephone. You send your request for a particular video or bit of information to a computer somewhere in the Tor network. This computer then relays that information on to another computer somewhere else in the network. Once again, this computer simply relays your request onwards to yet another machine. This third machine in the game of telephone then requests the information you want to view and sends it back to you along a similar, disjointed path.
>
> Breaking up the request in this way means that different people can see different parts of what you are viewing online, but it is exceptionally difficult, although not impossible, for any one person to connect all the dots to pinpoint who you actually are. [Citation.] Your ISP, for example, which normally knows exactly what sites you are visiting, can only see that you are sending a request to the first computer in the network. On the other end of things, the website can tell a lot about the computer that is accessing their content, but this information does not relate to your computer, instead linking to the last of the three computers in the game of telephone. The computers in the relay system know about their neighbour, but no more than that. The first link knows you and the middle computer, but not the end computer or the content viewed. The middle link knows the first computer and the end computer, but not you or the destination of your request. The end computer knows the destination and the middle computer, but not who you are. Layered onto this broken routing of your request is the heavily encrypted signal that prevents data flowing across the Tor network from being accessible to prying eyes.

Jardine, *Dark Web Dilemma*, at 2.

Tor describes itself and its mission in much the same way:

> Using Tor protects you against a common form of Internet surveillance known as "traffic analysis." Traffic analysis can be used to infer who is talking to whom over a public network. Knowing the source and destination of your Internet traffic allows others to track your behavior and interests. . . .
>
> Tor helps to reduce the risks of both simple and sophisticated traffic analysis by distributing your transactions over several places on the Internet, so no single point can link you to your destination. The idea is similar to using a twisty, hard-to-follow route in order to throw off somebody who is tailing you—and then periodically erasing your footprints. Instead of taking a direct route from source to destination, data packets

> on the Tor network take a random pathway through several relays that cover your tracks so no observer at any single point can tell where the data came from or where it's going.

Tor, *About Tor*, https://www.torproject.org/about/overview.html.en. The idea of "using a twisty, hard-to-follow route in order to throw off somebody who is tailing you," then "periodically erasing your footprints," certainly sounds appealing when the "somebody . . . tailing you" is a faceless menace. But "Tor is basically a dual-use technology": the anonymity it grants may allow some users to "voice contrary points of view against despotic regimes," while at the same time allowing others to access "the seedy underbelly of the Internet"—"illegal drug and weapon markets," along with "child abuse imagery" and "pedophilia rings." *See* Jardine, *Dark Web Dilemma*, at 2, 4–5, 7. And in more "open" countries, where citizen rights enjoy "constitutional and legal protections," "the need to use a full-blown anonymity program such as Tor" is low—that is, "unless people are engaged in outright illegal activities." *Id.* at 7.

There's one more critical note regarding Tor's service and structure. Personal-jurisdiction analysis is often conducted using commercial metrics: How many employees does the company have in the state? How many stores? How many online orders originated in the state, for how many sales dollars? Those metrics won't work for Tor. Tor claims "paid staff and contractors of around 35 engineers and operational support people," but allows that it has "many volunteers all over the world who contribute to [its] work." *See* Tor, *About Tor*, *Jobs*, https://www.torproject.org/about/jobs.html.en. (Tor lists nearly 100 "Core Tor People" on its website, but provides no states—or even countries—of residence, and some "Core Tor People" appear to be identified only by pseudonyms or handles.) And while Tor's funding comes "in part" from "government grants and contracts," it also comes from "individual, foundation, and corporate donations." *See id.* But given that Tor describes itself as "a group of volunteer-operated servers" whose "users employ [the Tor] network by connecting through a series of virtual tunnels rather than making a direct connection," *see* Tor, *About Tor*, https://www.torproject.org/about/overview.html.en, the most critical questions, for jurisdictional purposes, are about Tor's users and the "tunnels" they create: How widespread is Tor? Where are its users located? And where do these "tunnels" run?

The nature of Tor's services make these questions uniquely difficult to answer. After all, Tor's very purpose is to *hide* the locations and activity of its user network. But by its own metrics, Tor estimates, on average, between 350,000 and 400,000 "directly connecting users from the United States" over the past three months. *See* Tor, *Tor Metrics: Users* (select "United States" from the "Source" dropdown), https://metrics.torproject.org/userstats-relay-country.html. Given that Utah accounts for just under 1% of the U.S. population—and without any reason to believe that Utahns use Tor more or less frequently than citizens of any other state—those numbers suggest that between 3,000 and 4,000 Utahns use Tor *each day*. *See also, e.g.*, Karsten Loesing, *Counting daily bridge users*, Tor Tech Report 2012-10-001 (Oct. 24, 2012) (explaining that the work done by the Tor Metrics Project is meant to measure "how many people use the Tor network on a daily basis" and explaining its methodology).

The questions presented by Tor's Motion to Dismiss—questions about jurisdiction and immunity for a vast international anonymizing network—are no doubt important ones. But those questions can't be answered by simply analogizing to entities that operate mail-order catalogues or marketing websites or message boards. Simply put, Tor can't escape liability simply by labeling itself an "internet company." Tor's network includes thousands of Utahns each day, creating "tunnels" and passing information through Utah-based computers. And while information about the physical location of Tor "relays" and "bridges" isn't publicly available, Tor encourages its users to "consider running a relay to help the Tor network grow," *see* Tor, *Volunteer*, https://www.torproject.org/getinvolved/volunteer.html.en, and even offers to "assist [Tor] relay operators" in securing "qualified legal counsel" if they "get in trouble for running a Tor relay," *See* Elec. Frontier Foundation, *Tor Challenge*, *Legal FAQ*, https://www.eff.org/torchallenge/faq.html. Even a cursory search of Tor's relays strongly suggests the presence of Tor relays in

Utah. *See* Tor, *Tor Metrics: Relay Search* (conduct a "Simple Search" for "Utah"), https://metrics.torproject.org/rs.html#search (identifying active relays nicknamed "UnivUtah0" and "UnivUtah1," both of which are associated with the following "Host Name": tor.coe.utah.edu).

Tor wants to be everywhere, because its user network is, in many respects, its product: "As Tor's usability increases," the company explains, "it will attract more users, which will increase the possible sources and destinations of each communication, thus increasing security for everyone." Tor, *About Tor,* https://www.torproject.org/about/overview.html.en. And given the nature of Tor's product, this action can't be waved away by insisting that Tor is too amorphous to be sued anywhere or that Tor is nothing more than a content re-publisher.

Governing Standard

In considering a Rule 12(b)(6) motion to dismiss, a court will not "weigh potential evidence that the parties might present at trial," but asks instead "whether the plaintiff's complaint alone is legally sufficient to state a claim for which relief may be granted.'"[4] And in answering that question, a court must "accept as true all well-pleaded factual allegations in a complaint and view these allegations in the light most favorable to the plaintiff."[5]

Argument

I. Utah Has Personal Jurisdiction over Tor.

A nonresident defendant is subject to personal jurisdiction of a forum-state court if two conditions are met: (1) laws of the forum state render jurisdiction legitimate, and (2) the exercise of that jurisdiction does not offend the Fourteenth Amendment's due-process clause. *See Soma Med. Int'l v. Standard Chartered Bank*, 196 F.3d 1292, 1295 (10th Cir. 1999). Utah's long-arm statute must be interpreted broadly "so as to assert jurisdiction over nonresident defendants to the

[4] *Smith v. United States*, 561 F.3d 1090, 1098 (10th Cir. 2009) (quoting *Sutton v. Utah State Sch. for Deaf & Blind*, 173 F.3d 1226, 1236 (10th Cir. 1999)).

[5] *Id.*; *see also, e.g., Peterson v. Jensen*, 371 F.3d 1199, 1201 (10th Cir. 2004) (noting that Rule 12(b)(6) motions to dismiss are generally disfavored).

fullest extent permitted" by the due-process clause. *See* Utah Code § 78B–3–201.[6] Given the breadth of Utah's long-arm statute, the Utah Supreme Court itself "frequently make[s] a due process analysis first because any set of circumstances that satisfies due process will also satisfy the long-arm statute." *See SII MegaDiamond, Inc. v. Am. Superabrasives Corp.*, 969 P.2d 430, 433 (Utah 1998).

The due-process clause is satisfied only when "minimum contacts" exist between defendant and the forum state, *see World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286, 291 (1979), and that "'minimum contacts' standard may be met in two ways"—a court may assert specific jurisdiction over a nonresident defendant who has purposefully directed his activities at forum state residents, or it may assert general jurisdiction over a defendant whose business contacts with the state are continuous and systematic, *see OMI Holdings, Inc. v. Royal Ins. Co. of Canada*, 149 F.3d 1086, 1090–91 (10th Cir. 1998).

While a plaintiff bears the burden of establishing personal jurisdiction over a defendant, *see id.* at 1091, during the "preliminary states of litigation," a plaintiff needs only "establish a prima facie case that jurisdiction exists," *see Wenz v. Memory Crystal*, 55 F.3d 1503, 1505 (10th Cir. 1995). And when factual disputes arise in a personal-jurisdiction analysis, those disputes are resolved in the plaintiff's favor. *Id.*

A. General Jurisdiction

In its motion to dismiss, Tor characterizes itself as "an internet company" that operates "[a] web site," *see* Mot. to Dismiss 7–8 [Dkt. 13], and argues that it is therefore subject to general jurisdiction in Utah under Tenth Circuit law only if it "deliberately directed its message to an audience in [Utah] and intended harm to [the Seavers] occurring primarily or particularly in

[6] *See also, e.g.*, *Starways, Inc. v. Curry*, 980 F.2d 204, 206 (Utah 1999) ("We have held that the Utah long-arm statute 'must be extended to the fullest extent allowed by due process of law.'") (quoting *Synergetics v. Marathon Ranching Co.*, 701 F.2d 1106, 1110 (Utah 1985)); *Concur-Texas, LP v. Duradril, LLC*, No. 2:14-cv-218-BCW, 2014 WL 5682504, at *3 (D. Utah Nov. 4, 2014).

[Utah]," *see id.* at 7 (quoting *Shrader v. Biddinger*, 633 F.3d 1235, 1241 (10th Cir. 2011)). Put simply, Tor maintains that it "does not have continuous and systematic contacts such that it is at home in Utah." *Id.* at 8.

A handful of personal-jurisdiction cases are cited frequently in Utah federal district court: *Soma*, a 1999 Tenth Circuit case; *Zippo*, a 1997 case in the federal district court for the Western District of Pennsylvania, which *Soma* relies on; and *Patriot Systems*, a 1998 Utah federal district court case that cites *Zippo* and, in turn, is cited by *Soma*. *See Soma Med. Int'l v. Standard Chartered Bank*, 196 F.3d 1292 (10th Cir. 1997); *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997); *Patriot Sys., Inc. v. C-Cubed Corp.*, 21 F. Supp. 2d 1318 (D. Utah 1998). But as *Zippo* and *Patriot Systems* both point out, in the late 1990s "the development of the law concerning the permissible scope of personal jurisdiction based on Internet use [was] in its infant stages." 21 F. Supp. 2d at 1324 (quoting *Zippo*, 952 F. Supp. at 1123–24). These cases created and applied a sort of "sliding scale": when a defendant forms relationships with a forum state's residents "that involve the knowing and repeated transmission of computer files over the Internet," personal jurisdiction is proper, but not when a defendant simply "post[s] information" on a website accessible "to those who are interested." *Zippo*, 952 F. Supp. at 1123–24.

The Tenth Circuit took up this question again in earnest in 2011, in a case called *Shrader v. Biddinger*, which Tor relies upon heavily in its Motion to Dismiss. *See* 633 F.3d 1235 (10th Cir. 2011). *Shrader* didn't entrench or reject the "sliding-scale test" that appears in *Zippo* and *Soma*, but it did note that courts adopting the *Zippo* sliding-scale test "tend to employ it more as a heuristic adjunct to, rather than a substitute for, traditional jurisdictional analysis." *Id.* at 1242 n.5.

Tor is more than a company operating a website that is accessible in Utah. As Tor's own website and metrics demonstrate, Tor users do more than passively gather information from Tor's website. In fact, they do more than engage in commercial transactions through Tor's website. When a Tor user downloads the Tor browser, the user does so for a uniquely *active* reason—to access Tor's network of "tunnels," which allow users to send and receive information anonymously. Though Tor is specifically designed to mask the geographic locations of its users and relays, the sheer number of daily U.S. users—350,000 to 400,000—provides *prima facie* evidence that the Tor network is active and operational in Utah.

The Seavers acknowledge that, with respect to general jurisdiction, this question is a unique one. Tor is not a brick-and-mortar company with operations in another state but a website that makes it accessible to Utah consumers. Tor's product *is* its network—its network of users, relays, and bridges, which provide its promised anonymizing effects as information moves along a deliberately "twisty, hard-to-follow route," "periodically erasing [the user's] footprints." At the very least, this complex and important question merits discovery into the relationship between Tor's services and Utah as a forum state.

B. Specific Jurisdiction

Similarly, Tor argues that it is not subject to specific jurisdiction because "there are not facts that suggest that Tor had some connection to Utah related to [the Seavers'] alleged injuries." *See* Mot. to Dismiss 9 [Dkt. 13]. The critical questions, with respect to specific jurisdiction, are whether Tor "purposefully directed its activities" at Utah residents and whether the Seavers' injuries "arise out of" Tor's Utah-related activities. *Dudnikov v. Chalk & Vermillion Fine Arts, Inc.*, 514 F.3d 1063, 1071 (10th Cir. 2008).

With respect to the first question, the "purposeful direction" element "can appear in different guises" depending on the nature of the case. *See id.* But the "shared aim" of this element is "to ensure that an out-of-state defendant is not bound to appear to account for merely 'random, fortuitous, or attenuated contacts' with the forum state." *Id.* (quoting *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 472 (1985)).

Tor's contacts with Utah are not random, fortuitous, or attenuated. Again, Tor is a unique entity: it does more than market its product to Utah consumers—it urges users in Utah to *incorporate themselves* into Tor's product. And the results of this effort are entirely predictable: Tor grants access "the seedy underbelly of the Internet"—to "illegal drug and weapon markets," "child abuse imagery," and "pedophilia rings," *see* Jardine, *Dark Web Dilemma*, at 2, 4–5, 7—and it was access to this "seedy underbelly" that caused the Seavers' harm here.

Put simply, the chain of commerce that moved potent synthetic opioids from clandestine Chinese laboratories into the hands of middle-school students in Park City, Utah was possible only because of Tor's anonymizing service. One recent study concluded that "the most common uses for websites on Tor hidden services are criminal, including drugs, illicit finance and pornography involving violence, children and animals." *See* Daniel Moore & Thomas Rid, *Cryptopolitik and the Darknet*, 58 Survival: Global Politics & Strategy 1, 21 (2016). In fact, "[a] wide variety of drugs—both pharmaceutical and otherwise—constituted the single most common commodity within the Tor darknet." *Id.* at 23.

As the Seavers allege, the drugs that killed their son did so only because AlphaBay made an illicit transaction possible—and AlphaBay could do so only because of Tor's anonymizing services. Tor knows that its network is flooded with illicit drugs, it knows that its service makes those drugs available to anyone who downloads its browser, and it knows that thousands of Utahns—including minors—will use its network to buy, use, and distribute those drugs. Despite this, Tor purposefully directs its efforts into Utah—not just to provide Utahns with information or content created by some other third party, but to invite Utahns to become part of its product by participating in the Tor network.

Again, this is a novel question, as Tor—and its network-of-users product—should not be treated the same as an online retailer or bulletin board. But during the "preliminary states of litigation," the Seavers need only "establish a prima facie case that jurisdiction exists," *see Wenz v. Memory Crystal*, 55 F.3d 1503, 1505 (10th Cir. 1995). And given that any factual disputes here must be resolved in the Seavers' favor, *see id.*, Tor's motion to dismiss for lack of personal jurisdiction should be denied.

C. Fairness

Finally, Tor mentions an additional layer of personal-jurisdiction analysis: even if other jurisdictional requirements are met, a court "must still inquire whether the exercise of personal jurisdiction would offend traditional notions of fair play and substantial justice." *See* Mot. to Dismiss 9–10 [Dkt. 13] (quoting *Shrader*, 633 F.3d at 1240). Tor lists a number of factors that may be considered in a "fairness" determination, but then states that "it is unnecessary for the Court to analyze" the questions of "fair play and substantial justice," because "Tor does not have sufficient contacts with Utah" to satisfy the first stage of personal-jurisdiction analysis. *Id.* at 10.

The Seavers understand this absence of argument to mean that Tor does not contest that the balance of these factors tip heavily in the Seavers' favor. Given the amorphous nature of Tor's services and the resources available to it, Tor faces no unique burden in defending itself in Utah. Meanwhile, the remaining stakeholders—Utah, the Seavers, the interstate judicial system, and the framework of fundamental social policies—all favor resolution of this dispute in Utah, where the opioids arrived, where they were distributed, where they led to the death of the Seavers' son, and where the subsequent investigation occurred. *See Dudnikov*, 514 F.3d at 1080. This case should move forward here.

II. Tor Is Not Immune to Suit Under the Communications Decency Act.

Tor's second argument is that the Seavers' claims "are barred by the Communications Decency Act" (CDA), which, Tor argues, keeps "computer service providers" from being held liable "for information originating with a third party." *See* Mot. to Dismiss 11 [Dkt. 13] (quoting *Silver v. Quora, Inc.*, 666 F. App'x 727, 729 (10th Cir. 2016)). The CDA's immunity rule, as Tor states it, is this: "A person who is harmed by *a website's publication* of user-generated content may sue the third-party user who provided the content, 'but not the interactive computer service that enabled them to publish the content online.'" *Id.* (quoting *Doe v. MySpace, Inc.*, 528 F.3d 413, 418 (5th Cir. 2008)).

Again, Tor's argument hinges on a peculiar characterization of its own services. The CDA's goal is a simple one: it protects interactive-computer-service providers from being "treated as the publisher or speaker of any information provided by another information content provider." *See* 47 U.S.C. § 230(c)(1). If you run a question-and-answer website, for example, and a poster makes defamatory comments about a business, you cannot be held liable for simply providing the forum for those comments to be made. *See Silver v. Quora, Inc.*, 666 F. App'x 727, 728 (10th Cir. 2016). Or, if you operate a website that disseminates stock-quote information, and you post to the internet an inaccurate stock quote created by some other content provider, an aggrieved plaintiff must seek relief from the third-party content provider—not the website operator. *See Ben Ezra, Weinstein & Co., Inc. v. America Online, Inc.*, 206 F.3d 980, 983 (10th Cir. 2000).

CDA immunity is much narrower than Tor suggests. One limitation is that CDA immunity is available only to "interactive computer service providers"—and an entity qualifies for that label only if it "provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet." *See* 47 U.S.C. § 230(f)(2). A website operator may qualify, for example, because the operator allows users to access "a computer server, namely, the server that hosts the web site." *See Universal Commc'ns Sys., Inc. v. Lycos, Inc.*, 478 F.3d 413, 419 (1st Cir. 2007). Tor claims to be an "interactive computer service provider," at least in part because it allows users to download a "Tor Browser." *See* Tor, *Projects: Tor Browser*, https://www.torproject.org/projects/torbrowser.html.en. But unlike a website, which is simply a gateway through which a user contacts a host server, Tor is designed to do something much different—to actually alter the relationship between the user and the rest of the world by anonymizing the user, by "bouncing [the user's] communications around a distributed network of relays run by volunteers all around the world." *Id.* That "bouncing," in turn, prevents others from "watching [the user's] Internet connection from learning what sites [the user] visit[s]," prevents sites "from learning [the] physical location" of the user, and even "lets [the user] access sites which are blocked." *Id.* In short, Tor's service is wildly different than the services offered by "interactive computer service providers," as defined by the statute itself.

A second limitation is that CDA immunity is available only when a defendant's liability is premised on its actions as a "publisher or speaker." *Silver*, 666 F. App'x at 729. The purpose of the CDA is "to encourage service providers to self-regulate the dissemination of offensive material over their services," and to do so, the CDA "forbids the imposition of publisher liability on a service provider for the exercise of its editorial and self-regulatory functions." *See Ben Ezra*, 206 F.3d at 986 (citing *Blumenthal v. Drudge*, 992 F. Supp. 44, 52 (D.D.C. 1998). Unlike the Q&A service or stock-quote website described above, Tor's liability in this case isn't premised on some sort of re-published information. Tor's liability is based on its facilitation of a brazen, illicit marketplace—Tor's anonymizing service made possible the transaction that killed the Seavers' son. The CDA does not shield Tor from that theory of liability.

The third limitation is that the CDA creates liability only when "another information content provider provided the information at issue." *See Silver*, 666 F. App'x at 729 (internal quotations marks omitted); *Accusearch*, 570 F.3d at 1196. When "a typical Internet bulletin board is neutral with respect to the content's offensiveness," for example, it may be able to claim CDA immunity. *See Silver*, 666 F. App'x at 729; *Accusearch*, 570 F.3d at 1199. On the flipside, if a service provider "specifically encourages development of what is offensive about the content," the CDA grants no immunity. As the Seavers allege in their Complaint, there's nothing "neutral" about Tor: its anonymizing service courts illegality and vice. Tor is thus barred from CDA immunity under all three limitations described in *Silver* and *Accusearch*.

The CDA exists for specific reasons: to protect Facebook for being sued for a user's posts, for example, or to keep Gmail from being sued for a defamatory statement that travels by email.

Those protections don't apply to Tor here. Tor's CDA argument thus fails, and its Motion to Dismiss on this basis should be denied.

III. Plaintiffs' Injuries Are Traceable to Tor.

Finally, Tor argues that it is "a completely neutral party," and that any injury the Seavers suffered is "not traceable or attributable to Tor." *See* Mot. to Dismiss 14–15 [Dkt. 13]. Tor's analysis ends there.

Tor offers little explanation as to how—at the motion-to-dismiss stage, where all well-pleaded factual allegations are presumed to be true, *see Ashcroft v. Iqbal*, 556 U.S. 662 (2009)—the Court could conclude that the Seavers' injury is "not traceable or attributable to Tor." It's unusual to even raise the argument at the motion-to-dismiss stage, as the "traceability of a plaintiff's injury"—whether a particular defendant's breach caused the harm at issue—"raises an issue of fact 'to be submitted to the jury for determination.'" *Harline v. Baker*, 912 P.2d 433, 439 (Utah 1996) (quoting *Mitchell v. Pearson Enters.*, 697 P.2d 240, 245 (Utah 1985)); *see also Mahmood v. Ross*, 1999 UT 104, ¶ 22, 990 P.2d 933 ("Proximate cause is generally determined by an examination of the facts, and questions of fact are to be decided by the jury."). In other words, the question Tor takes up in the third section of its Motion to Dismiss would be premature even if it were raised at summary-judgment stage, much less in a Rule 12(b)(6) motion.

Tor does seem to suggest that the Seavers' Complaint lacks specificity or clarity about Tor's role in their son's death. But the Seavers' theory is straightforward. The Seavers understand that powerful synthetic opioids made their way from a Chinese laboratory into the hands of several Park City teenagers. The path those drugs traveled exists only because of the "online bazaar" called AlphaBay, and AlphaBay existed only because of Tor. *See* Andy Greenberg, Wired, *The Biggest Darkweb Takedown Yet Sends Black Markets Reeling* (July 14, 2017), https://www.wired.com/story/alphabay-takedown-dark-web-chaos/. As one report explained in July 2017, just after AlphaBay was shuttered following a federal investigation, "Sites like AlphaBay . . . aren't normal websites, but so-called 'hidden services' designed to be accessed only with the anonymity software Tor . . . ." *Id.*

Tor is a named in this action for a simple reason: were it not for Tor's anonymizing service, the synthetic opioids that killed the Seavers' son would never have made it into the hands of Park City middle schoolers. Tor is free, as litigation progresses, to argue that others share the blame for G.S.'s death. But that theory has no place in a motion-to-dismiss analysis. Tor's "traceability" argument therefore fails, and the Court should deny its Motion to Dismiss on these grounds.

Conclusion

Tor's anonymizing service is more than a passive message board or a commercial portal. Tor made AlphaBay possible, and a transaction that could only have occurred on AlphaBay cost the Seavers' son his life. This Court can rightfully exercise personal jurisdiction over Tor, Tor is not entitled to CDA immunity, and the Seavers' Complaint traces the path from Tor's wrongdoing to the harm they suffered. Tor's Motion to Dismiss should therefore be denied.

Dated: December 5, 2018.

JONES WALDO HOLBROOK & McDONOUGH PC

By: */s/ J. Angus Edwards*
Jeffrey D. Gooch
J. Angus Edwards
JONES WALDO HOLBROOK & McDONOUGH PC

Attorneys for the Seavers

CERTIFICATE OF SERVICE

I hereby certify that on December 5, 2018, I caused to be delivered, via the court's electronic filing system, email, or otherwise by first class mail postage prepaid if needed, a true and correct copy of the foregoing **PLAINTIFF'S OPPOSITION TO TOR'S MOTION TO DISMISS**, to the following:

Vincent J. Velardo (velardo@litchfieldcavo.com)
Greg Soderberg (soderberg@litchfieldcavo.com)
LITCHFIELD CAVO LLP
420 E. South Temple, Suite 510
Salt Lake City, Utah 84111

Attorneys for The Tor Project, Inc.

By: *Annelie Furner*